PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F — A2

(11) International Publication Number: WO 98/22914

(43) International Publication Date: 28 May 1998 (28.05.98)

(21) International Application Number: PCT/US97/21809

(22) International Filing Date: 20 November 1997 (20.11.97)

(30) Priority Data:
60/031,283 20 November 1996 (20.11.96) US

(71) Applicant: TECSEC, INCORPORATED [US/US]; Suite 220, 1953 Gallows Road, Vienna, VA 22182 (US).

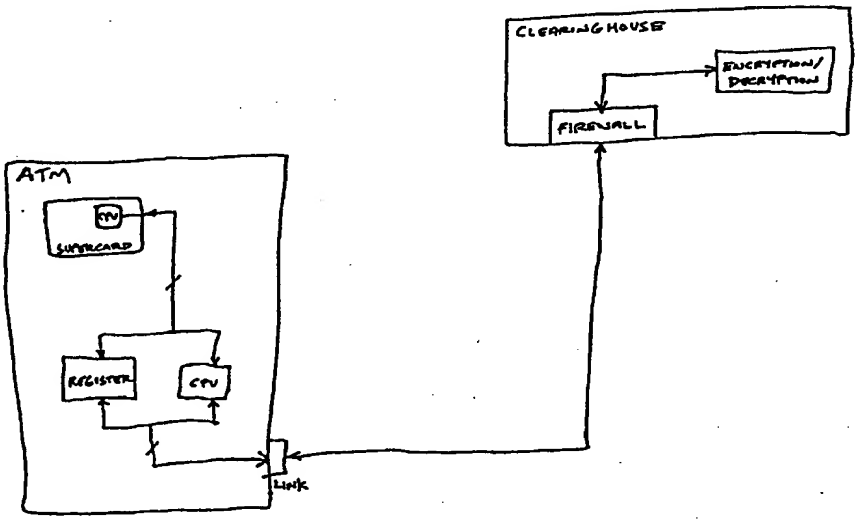
(72) Inventors: WACK, Carl, J.; Clarksburg, MD (US). SCHEIDT, Edward, M.; McLean, VA 22101 (US). HERSHLOW, John, H.; Berkeley, NJ 08721 (US).

(74) Agent: CHAMPAGNE, Thomas; Rabin, Champagne & Lynt, P.C., Suite 1111, 1725 K Street, N.W., Washington, DC 20006 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: CRYPTOGRAPHIC MEDIUM



(57) Abstract

A cryptographic medium including embedded metallic particles. The particles provide a unique signature when the card is exposed to a radio frequency signal. The medium includes programming and storage capability, so that protocols for different types of transactions may be stored on the medium, along with personal information associated with the user of the token. The token may take the form of a plastic card, which includes an electronic module fabricated using a multi-chip module design and including the programming and storage capability. The design allows greater computing and storage capacity on the card. At least the electronic module is encapsulated in a plascon material, giving the overall card a more physically secure construction.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

CRYPTOGRAPHIC MEDIUM

FIELD OF THE INVENTION

The present invention relates in general to a medium used for performing transactions. In particular, the present invention relates to a medium used for performing secure transactions, such as banking or other commercial transactions.

BACKGROUND OF THE INVENTION

Currently, activity in the area of smart cards has been driven primarily by the need to protect the telephone industry. Cellular telephones in particular are subject to fraudulent billing, at worst, and refusal to pay problems at best; in any event, the losses are measured in the millions of dollars per day in N.Y. City alone. In Europe, the GSM cellular system took action and instituted the telephone card system, which required the use of a card to prepay the call or cash debit a prepaid account. This approach corrected the problems with the telephone charge system to some degree. However, the criminal element moved its attentions to different methods, from cloning (counterfeiting) the telephone to the attacking (fraudulent use) the prepaid cards. These cards, designed for telephone use, are for the most part decrement-only cards, or prepaid cards which are used and then thrown away. This type of card represents approximately 90% of the total number of "smart" cards generated in the world.

Industry standard cards, having been developed with the phone card application in mind, took advantage of the ready accessibility of semiconductor memory chips, and the card manufacturers, seeing a disposable market as being ideal, decided to make the "smart card" as an inexpensive throwaway. By making as few changes in existing products as possible, a method of billing phone calls only required the insertion of a small semiconductor die, which was then connected by wire to the minimum of contact points, into a card (paper or plastic). The very requirements which were necessary for the one application drove the rest of the industry. The poor physical security of a die embedded into a 25mm sq. well milled in the plastic card also meant that the lifetime of the card

could be measured in days. Still, this continued to be suitable for the telephone industry.

Security as a whole, has been under review at all levels of the information infrastructure. Computers, which are used to access control to information, to physical locations, and to special areas are also under review. All software solutions for security are all too easily compromised. A token device to be held by the individual user was required.

Currently, the widespread adoption of these concepts is evident by the need for an average individual to carry a half-dozen cards, or more. What was once a simple need and requirement, has over time developed into an accepted practice. The downside of the widespread adoption of cards is the sheer number of cards required by an individual.

Also involved is the relationship of each individual with the computer-aided environment. Microsoft, and others in the computer software business, have gone to great lengths to encourage each person to rely, to an ever-greater degree, with a computer at home and the computer in the workplace. Industry has also invested great sums of money to take advantage of the efficiencies and workflow improvements provided by the computer.

Available computer software includes hundreds of applications, which would at first glance seem benign, but may render users vulnerable and even whole industries are now blurred with respect to the computer. For example, where or what is a "virtual point of presence"? Banking in particular, which as an industry has traditionally made its profit margins on services and the need for customers to visit, or at least exchange paper (money, stocks, bonds, etc.), have a serious problem with the provision of these traditional banking services using software, through on-line companies like Microsoft and Intuit.

In recent years security of information within the banking community has been deemed as only necessary during the transmission of information over special leased "private network" lines. The banks have placed cryptographic link devices between one point of communications and another, e.g., bank to bank. In the original scheme of things this worked. Banks were primarily paper houses and the only transfer of information was in the form of messages or specific types

of information, having format and structure, but still just between the banks and ultimately to the Federal Reserve or Treasury Department.

As computers reached the desktop in size and capability, the banks, eager to become efficient, began to connect more and more employees and service groups together. The interoffice connection was considered "safe" largely because all of the connectivity was internal to the bank and relatively isolated.

As the banks branched out to reach customers so did the banks network facility reach out and expand the ability of the bank employees and executives to communicate with one another. Still, the security solution was defined as only being necessary for those transactions between facilities, and this requirement could be satisfied by the communications link equipment. However, the growth of the intra-bank communications paths reached a degree of complexity and completeness which was not entirely expected. The hardware engineers had succeeded, everyone could talk electronically to everyone else about anything. However, all information is not equal and something must be done to control the flow of information proportional to the need to know access of the various individuals within the bank. Customer data needed to be protected from those employees who did not need to know about account balances. Merger and acquisition trader information could not be allowed to be available to the teller at the computer-based drive in window.

Moreover, as the interconnectivity of the bank as an institution increased, the availability of information became more and more accessible to more and more people. Encryption of the links between facilities, while still necessary to protect the information being sent from one location to another, did not provide the separation of information required. Other examples of the need for the separation of information were established with the passage of the Privacy Act of 1974. This law made it mandatory for the confidential information acquired either by employers, or banks or doctors and the like, be held in confidence and protected from unauthorized or inappropriate access.

To further complicate the information distribution pool, is the rising demand to provide banking services and products to the customer via EDI or the Internet. Current use of hardware link devices does not allow for protection of the information moving from address to address or person to person within the

network of a given bank or organization. Nor does the process of protecting the link of communications provide any confidentiality to the information moving within the link.

The same situation is true for information moving from an Automated Teller Machine (ATM) to a bank or clearinghouse. The industry as a whole has been trying to resolve this and has submitted a specification: "The Secure Electronic Transaction Specification" or SET. This specification provides for the protection of information in transmission from one EDI position to another, that is, from merchant to bank or ATM to clearinghouse. This specification, however, is not intended to protect the information itself, just the path. It is up to the functional owner of the information to provide security to the information. To this problem is offered this solution.

It is the parallel needs of these circumstances which demands an overall solution. The deficiencies present in conventional cards which make them unsuitable as a solution are many. For example, each has a small die size defined by the 25mm well or hole in the card. Further, the practice of mounting the die in a drop of epoxy exposes it to environmental, logical, and physical abuse. This type of product offers limited physical and logical security. The result is minimal functionality and memory capacity available if the semiconductor industry is bound by the 25mm square definition imposed by the card industry. An additional limitation is the dependence of the industry on existing solutions in cryptographic security, and the overall misapplication of these generic solutions to a very specific task.

On the logical issue, conventional cards have, on the whole, tried to use a public/private key approach for controlling access to the card information. This has had its limitations for several reasons. First, the public/private key process requires a separate co-processor to accomplish the actual computations, and this co-processor can take up to 40% of the total die size and also of the limited space in the card well. Further, the computations of public/private key are time consuming and each effort provides an unwelcomed delay in performance. The issue of protection of an individual's private key is often overlooked, that is, the entire security scheme is dependent on the private half of the key remaining a secret.

Plastic cards have been in use for a number of years. Plastic is inexpensive, allows for shaping, printing, embossing, and for the addition of a strip of magnetic tape. However, all of these common characteristics also enable misuse when a plastic card is applied to a financial or credit application. Credit card fraud is a major problem precisely because of the ease of duplication of the plastic card.

What is required is a method or process to provide a unique characteristic to the plastic card/material which is also inexpensive so as to not impact the ubiquitous use of the product, and at the same time defeat the misuse of the device in financial applications.

SUMMARY OF THE INVENTION

The approach of using a small 25mm sq. hole in a card was defined by the physics of the semiconductor die. The overall dimensions of a single memory die is measured in width, length, and height. The length and width are fixed and immutable. However, the average die is between 20 and 25 mils thick. And of that thickness, approximately 12 to 17 mils is occupied by the alumina substrate necessitated by the photoetching process of semiconductor manufacturing. By putting together a multi-chip module (MCM) design which provides a high degree of density and capability, and then encapsulating the MCM in a plascon material, similar to the material currently used in the standard semiconductor manufacturing process, to provide stability, a thinning process can be executed which renders the thickness of the entire module to between 6 and 10 mils in thickness. This very thin product also takes on a very high degree of flexibility, analogous to aluminum foil and aluminum plate. This thinning removes the need for the 25mm limitation found in all other industry products. In fact, 80% of the area of the plastic card can be used to house electronic components.

Because of the plascon, the flexible MCM is completely sealed from outside environmental contaminates. The resultant module can be laminated within two outer layers of plastic and actually be reused if the outer housing should be damaged by accident or misuse.

This provides an improvement in security, which in existing cards is minimal in the physical sense. The unprotected die of memory or processor

functions is currently wire bonded to an ISO-specified metal contact material (see ISO Std. 7816-2 / Physical Specifications and –3 / Electrical Specifications). As such, the die is open to probing, attachments, or any other type of physical analysis. Further, when you flex the current industry standard card, the imbedded die jumps up and off of the card like a flea.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 a block diagram showing an exeplary use of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Metallic material can be shaped into very small particles. Slivers of metal of varying lengths have a particular characteristic when used as an antenna for radio frequency. When the metal length and the wavelength of the radio frequency are the same, the metal material resonates, or more accurately reflects the signal in a very efficient manner. The mixing of very small, sub-micron bipolar antennas, that is, metal particles in the plastic slurry at the time of manufacturing, would generate a naturally random disbursement of the metal particles in the resultant plastic card. This random placement of particles can then be illuminated with a very low level RF signal which reflects a unique pattern based on the physical position of the particles suspended in the material. This reflected pattern is unique for each card, unique to the frequency used to illuminate the card, and different depending on which portion of the card is used to compare patterns.

This unique physical signature can be used to assure the physical integrity of the card as well as the unique identity of the card because the disturbance of the particles, not only as individual particles but also in relationship to each other particle as a whole entity (this is a 3 dimensional event), is detectable.

In the case of credit cards or Automatic Teller Machines (ATM) applications, the card and its unique RF signature can be read at the time of insertion, very quickly, and the physical integrity and unique identification of the card is corroborated. The frequency at which the card is read may also change or be varied at what ever periodicity is desired. For example, on the first day of manufacture, the card is read in a stripe fashion much the same as a common

magnetic stripe is read today. However, this RF reading is made at an initial frequency of 10Ghz. The reflected signal is characterized and stored in a database along with the account number and name of the recipient of the card. At each reading of the card thereafter, not only can the initial reading be confirmed, the card can be read at another frequency to add to the initial characteristic database and can be used to check the same integrity and uniqueness. In a matter of days, the continuous use of the card would allow for check and counter-check against an immutable physical characteristic, assuring the issuer of the card that it had not been tampered with in any physical way.

The card of the present invention has two physical components, the plastic carrier or body of the card and the electronic module (approximately 1 square inch of semiconductor die, interconnected and embedded in plascon). The RF signature can be read on the module as a separate entity and/or combined with the signature of the card itself, to assure the relationship of the two devices is as originally intended. Moreover, if the card body or carrier should be damaged beyond the toleration level of the issuer or holder, the original card can be destroyed and the electronic module portion can be embedded into another card body, at which time a new signature would be read and used for future RF validation processes. This would allow continuous use of the content of the electronics, and reduce the replacement cost to the issuer of the cost of the plastic body or card.

A token device is consistent with Federal Information Publication System Bulletin #140-1. It is within this document that the concept is expressed that identification of an individual to a system should be token-based. The idea is that individual information should reside off of the computer system that is used for information sharing and in a platform that is separate and isolated from access by others on that system. This means that the token may be represented by a floppy disk, a PCMCIA card, or a smartcard. The limitations of function and capacity of other cards have restricted the application of this type of a system.

Tokens have been in use for a number of years. In fact, one of the problems in the security/access control market is the number of different tokens necessary in the day's events. A token (swipe card) is used to enter a garage area, another permits entry into a building, a third allows for access to a special

secured area, and yet another token is required for access to a computer terminal. In certain environments, the number of tokens may exceed a dozen. This situation is caused primarily by the development of each of the various systems under different manufacturers, each of whom, in trying to get the most out of a sale, insists on their own token. A common token for all functions has not been possible for lack of computational power and memory capacity.

The present invention with its 16-bit CPU and large (initially 1 Megabyte) memory capacity offers several significant parts to the overall solution set of problems associated with security and electronic transactions.

The 16-bit CPU offers the computational capability necessary not only to process large addressing schemes, but also to process a variety of protocols and the communications structures of different manufacturers. The card of the present invention can support large memory transfers and more importantly, can support multiple applications on a single card. The introduction of Constructive Key Management cryptography enables the card to enforce this application separation. Each functional owner of a memory segment or application can operate a completely different process of access and data storage, with the knowledge that it is not possible for any one else to have access to an inappropriate information object.

Such a card has been manufactured by Lockheed Martin, Sillcocks Plastics, and Secure Transaction Solutions using an Intel 80188EB CPU; 64k bytes of One Time Programmable processor instructions; 512k bytes of DRAM for memory buffer and scratchpad memory for CPU activity (program execution); 512k bytes of Electrically alterable program memory; and the associated latches and switches necessary to operate the card. Additional configurations may be utilized. The CPU addressing scheme allows for direct memory addressing of 32 megabytes of memory in various configurations of RAM and ROM consistent with the requirements of the various applications.

The plastic stock material from which the card is cut is impregnated with the sub-micron chaff material necessary for the RF ID process to operate. The RF Signature and ID process is thereby associated with the card (for example, the RF signature at various frequencies and various locations on the card).

The card is also capable of supporting magnetic stripe, printed information such as a 4-color photo, fingerprint, signature block, special symbols or logos, holograms, and other pieces of printed or attached information.

The basic operating system for the CPU may be installed in the EEPROM at the time of manufacture, or prior to manufacturing, at the EEPROM factory.

The card is assigned to a particular user, with a unique account number, and the RF ID is read and stored in non-volatile memory along with any other issuer / user-necessary information that might be desired, like a 4-color photo of the user (compressed and hashed), and a File Allocation Table (FAT) is created to allow the CPU to parse the memory sectors for later activation for additional applications. The user, upon receipt, will activate the card if received remotely, much as one does with conventional cards, and consistent with security practice if access is granted under a separate channel of distribution, e.g., telephone, U.S. Mail, or courier. The user can accept the offered Personal Identification Number (PIN) or select his/her own.

An exemplary use of the card of the invention is now illustrated, with reference to Fig. 1. The card is presented to an ATM. The RF ID is read from the card and its value is read into a register. The CPU of the card and the ATM exchange a series of signals to establish a common protocol. The card is capable of multiple protocols and therefore allows for a much greater degree of freedom of participation for the user.

Having achieved a common communications base, the ATM requests the PIN of the user of the card, which is stored in an encrypted form in the memory sector appropriate to that type machine, for example a *MOST, or Cirrus* transaction. The PIN is transmitted on-line to the respective clearing house via the dedicated SET-approved communications link, along with the previously-stored RF ID number. This information is sent to a clearing house firewall where the format of the information is screened for conformity. If it is acceptable, the packet is allowed to continue onward to the decryption area, where the information packet is decrypted using the indexing information bits in the header of the sent information along with the RF ID data to create a user key, which when combined with the database-stored component of a user access table generates the key to decrypt the actual packet. Within the packet are the credentials of the individual account,

the confirmation of the holder and card, and an audit of a predetermined number of past transactions which are relevant to this particular issuer. The past transactions are validated and the permission is sent to the ATM to proceed. The validation of past transactions includes the performance of several functions, the obvious update or correction if necessary, and also the assurance offered to the issuer that the message or content of encrypted data is large enough to assure no tampering or partial changes have occurred. The ATM then presents a list of actions which can be chosen by the user, and those selections are used as cryptographic splits to generate at the ATM an encrypted request/instruction which is sent to the clearing house. The screening process is repeated and if appropriate, the transaction is allowed. The updated (audit trail included) user packet is encrypted at the clearing house and sent back to the ATM to be entered on the user's card. No encryption occurred, on the card, in this particular transaction. In another protocol, or in a different application, encryption may be desired and desired to occur on the card. The powerful 16-bit processor and memory configuration of the card supports the choice.

Use of the card of the present invention in making a credit card transaction is now described. The card is offered to the merchant terminal. The terminal reads the RF ID value and stores it in a register. The card negotiates an exchange to determine correct protocol with the merchant device. The card, having a powerful 16-bit CPU, is capable of processing many different applications and protocols, and having achieved an acceptable communications link, also negotiates the highest baud rate that is mutually acceptable, up to 115,200 baud (currently). The merchant terminal requests on-line status with the respective clearing house and the combined value of the RF ID and the merchant membership number, along with the terminal ID number, are used to generate a unique key which is used to communicate and build a session key with the clearing house. The unique session key assures the participating merchant and the user of the card that the total transaction will be transmitted to the clearing house and the resulting answer will be encrypted using the identical components for key construction, assuring that the answer or acknowledgement can only be deciphered by the appropriate parties, i.e., the user and the merchant, at that

particular device. The information at the clearing house is decrypted and processed and the audited transaction is processed.

The card of the present invention may also be used to establish a secure Internet commerce relationship. A user of the Internet selects a Web page of a particular vendor. The page offers an opportunity to download transaction software. A click of the mouse and the transfer is complete. The software is sent as a serialized self-extracting executable file, which when selected will extract and install itself and present a screen that asks if now would be a good time to fill out the registration form for that particular vendor. This is also suggested to occur off-line. The registration form is filled out and all significant data is entered, including the type of payment, credit card number, etc. The software asks if the user wishes to take advantage of a Storage of Permissions Feature, which allows the user to store on the card, the permission/identifying splits that were generated by the vendor software. The user agrees and the card is presented and the information stored. The send button is selected and the automatically-encrypted bundle is sent back to the vendor of choice. The vendor receives the encrypted bundle and opens it. Recognizing the form/structure of the bundle, the encryption is automatically keyed with the serial number of the copy of the downloaded software, and the vendor firewall allows the bundle to pass to the processing area. The user, having gone back to the Web page, is now looking at the vendor catalog and selecting items for purchase, each of which has a number. It is the combination of these numbers and the number of the serialized software that generates the selected components of the split key encryption. All messages are protected and all communications are unique between the vendor and the user.

What is claimed is:

1. A cryptographic medium, comprising:
a plastic base;
metallic slivers embedded in random locations in the plastic base for providing a unique RF signature; and
an electronic module coupled to the plastic base, comprising
processing means, and
storage means.

2. The cryptographic medium of claim 1, wherein the plastic base includes a plascon material encapsulating at least the electronic module.

3. The cryptographic medium of claim 1, wherein the metallic slivers are formed in random sizes.

4. The cryptographic medium of claim 1, wherein the metallic slivers are formed in random, submicron sizes.

5. The cryptographic medium of claim 1, wherein the electronic module includes a central processing unit.

6. The cryptographic medium of claim 5, wherein the central processing unit is a 16-bit central processing unit.

7. The cryptographic medium of claim 1, wherein the electronic module includes storage memory.

8. The cryptographic medium of claim 7, wherein the storage memory includes user identification data.

9. The cryptographic medium of claim 8, wherein the user identification number is suitable for providing access to a financial account through use of an automated teller machine.

10. A method of forming a cryptographic medium, comprising:

a) forming a plastic base having a void therein, and metallic slivers embedded therein;

b) fabricating an electronic module using a multi-chip module design;

c) placing the electronic module within the void; and

d) encapsulating at least the electronic module in a plascon material.

11. The method of claim 10, wherein fabricating an electronic module includes fabricating a central processing unit.

12. The method of claim 11, wherein fabricating a central processing unit includes fabricating a 16-bit central processing unit

13. The method of claim 10, wherein fabricating an electronic module includes fabricating a storage memory.

14. A method of using a cryptographic medium in a transaction, comprising:

a) presenting a token at a transaction point;

b) reading physical characteristics of the token to obtain a signature of the token;

c) interpreting the signature to extract information; and

d) determining whether the transaction will proceed based on the extracted information.

15. The method of claim 14, wherein the physical characteristics of the token include the presence of metallic slivers included in the token.

16. The method of claim 15, wherein the signature of the token is a radio frequency signature.

17. The method of claim 14, wherein the extracted information is security information.

18. The method of claim 14, wherein the information is token user identification information.

19. The method of claim 14, further comprising reading data from the token.

20. The method of claim 19, wherein reading data from the token includes communicating with a processing unit disposed on the token to read the data stored in memory disposed on the token.

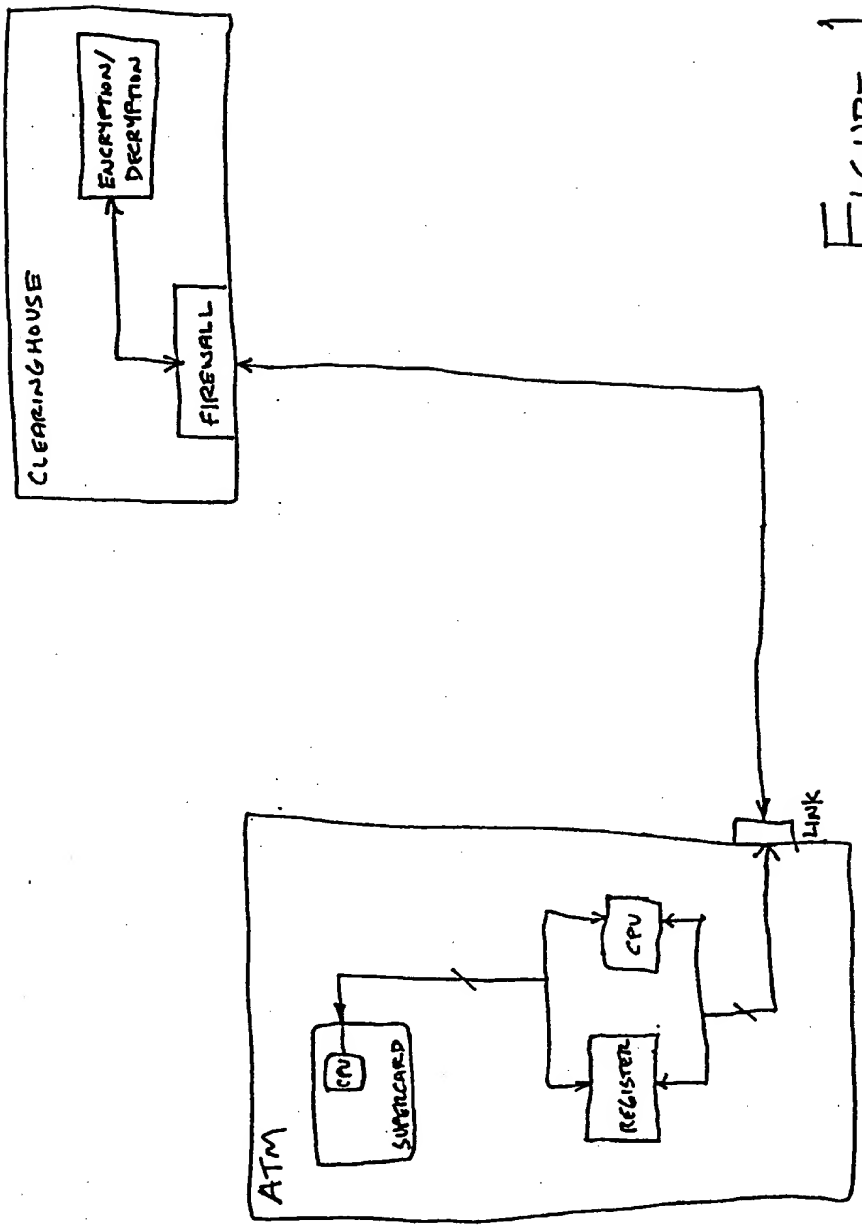

CLEARING HOUSE
ENCRYPTION/
DECRYPTION
FIREWALL
Link
ATM
CPU
REGISTER
SMARTCARD
CPU

FIGURE 1